Template - Logon from a risky IP address

Link to alert

**Description**

The single risky IP address that had either bad password or extranet lockout sign-in activities. This could be an IPv4 or an IPv6 address.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

User details

User:

Country or region:

Office:

**Alert details**

Activity:

Date:

Application:

Device:

IP address:

Location:

Authentication detail:

* Authentication method:
* Authentication method detail:
* Succeeded:
* Result detail:

ISP:

Severity:

**Remediation**

Confirm if the user has a VPN or Tor browser in use which would explain the alert.

Otherwise, reset the password to a strong password and ensure that MFA is enabled with two MFA methods.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***